STIC EIC 2100 Search Request Form

123844
26

Today's Date: 6/4/04

What date would you like to use to limit the search?
Priority Date: 11/29/2000 Other:

Name Minh Dieu Nguyen
AU 2137 Examiner # 79995
Room # PK2 4R20 Phone 3059727
Serial # 09/725272

Format for Search Results (Circle One):
PAPER DISK EMAIL

Where have you searched so far?
USP DWPI EPO JPO ACM IBM TDB
IEEE INSPEC SPI Other EAST

Is this a "Fast & Focused" Search Request? (Circle One) YES NO
A "Fast & Focused" Search is completed in 2-3 hours (maximum). The search must be on a very specific topic and meet certain criteria. The criteria are posted in EIC2100 and on the EIC2100 NPL Web Page at http://ptoweb/patents/stic/stic-tc2100.htm.

What is the topic, novelty, motivation, utility, or other specific details defining the desired focus of this search? Please include the concepts, synonyms, keywords, acronyms, definitions, strategies, and anything else that helps to describe the topic. Please attach a copy of the abstract, background, brief summary, pertinent claims and any citations of relevant art you have found.

- generate a first multivariable function
- generate a 2nd _____ by substituting the signer's id code into a 1st variable of the 1st function
- output 2nd function as a signing key for signer
- generate a random #, a 3rd function is obtained by substituting random # into a 2nd variable of 1st function
- output random # and 3rd function as a verification key for verifier

$f_1(x, y, z)$

$f_2 = f_1(\text{signer's ID}, y, z)$ = signing key for signer

$f_3 = f_1(x, \text{r.d}, z)$

random # + f_3 = Verif. key of verifier.

STIC Searcher Geoffrey St. Leger Phone 308-7800
Date picked up 6/4/04 Date Completed 6/4/4

Search and Information Resources Administration

File 348:EUROPEAN PATENTS 1978-2004/May W04
(c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040527,UT=20040520
(c) 2004 WIPO/Univentio

Set	Items	Description
S1	21768	(RANDOM? OR PSEUDORANDOM?)(3W)(NUMBER? ? OR NUMERAL? ? OR VALUE? ? OR DATA OR INFORMATION OR FIGURE? ? OR DIGIT? ? OR INTEGER? ? OR BIT? ? OR BYTE? ? OR CONTENT OR AMOUNT? ? OR QUANTIT???)
S2	9229	(SECOND? OR 2ND)(2W)(VARIABLE OR PARAMETER OR ATTRIBUTE OR LETTER OR PLACEHOLDER OR PLACE()HOLDER)
S3	8	S1(7N)S2(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR INCORPORAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING OR IN(1W)PLACE)
S4	589	S1(7N)(B OR Y)(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR INCORPORAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING OR IN(1W)PLACE)
S5	152	S4(100N)FUNCTION? ?
S6	4	S4(100N)(F(1W)(A()B OR X()Y))
S7	13402	(RANDOM? OR PSEUDORANDOM?)()(NUMBER? ? OR NUMERAL? ? OR VALUE? ? OR DATA OR INFORMATION OR DIGIT? ? OR INTEGER? ? OR BIT? ? OR BYTE? ? OR AMOUNT? ?)
S8	4443	F(1W)(A()B OR X()Y)
S9	17	S7(100N)S8
S10	1131	S7(10N)(B OR Y)
S11	7	S8(100N)S10

3/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

1012675
Method of loading a secret key of one device into another device
Verfahren zum Laden eines Geheimschlussels einer ersten Vorrichtung in eine zweite Vorrichtung
Methode pour charger une cle secrete d'un dispositif dans un autre dispositif
PATENT ASSIGNEE:
Setec Oy, (2544722), Suometsankaari 2, 01740 Vantaa, (FI), (Applicant designated States: all)
INVENTOR:
Hansson, Mika, Saviahonkatu 7, 11120 Riihimaki, (FI)
Rantala, Janne, Hyljekaari 1 E, 02260 Espoo, (FI)
Leiwo, Jussipekka, Lansantie 3E 52, 02610 Espoo, (FI)
LEGAL REPRESENTATIVE:
Holmstrom, Stefan Mikael et al (81962), Kolster Oy Ab, Iso Roobertinkatu 23, P.O. Box 148, 00121 Helsinki, (FI)
PATENT (CC, No, Kind, Date): EP 1331614 A2 030730 (Basic)
EP 1331614 A3 031112
APPLICATION (CC, No, Date): EP 2002396183 021210;
PRIORITY (CC, No, Date): FI 2012449 011212
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO
INTERNATIONAL PATENT CLASS: G07F-007/10
ABSTRACT WORD COUNT: 137
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; Finnish
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200331	668
SPEC A	(English)	200331	3872
Total word count - document A			4540
Total word count - document B			0
Total word count - documents A + B			4540

...SPECIFICATION first device via its input before the calculation or, alternatively, the first device can be arranged to generate it. If the first device generates the **second parameter** R2 itself, then this may be carried out for instance by utilizing a **random number** generator, which is **used** to generate a **random number** that fulfils given conditions and whose value is given to the **second parameter** R2.
The assumption in the exemplary case of Figure 1 is that the second parameter R2 remains known to the manufacturer of the device. Thusnot even the manufacturer of the device knows the secret key of the device afterwards. The device C1 comprises a **random number** generator for generating a **second parameter** R2 fulfilling given conditions. **Using** the secret key K stored in the memory and the second parameter R2, the processor P1 of the device C1 calculates the first parameter R1...

3/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

0661522
Encryption apparatus, communication system using the same and method therefor
Verfahren und Kommunikationssystem unter Verwendung einer Verschlusselungseinrichtung
Procede et systeme de communication utilisant un dispositif cryptographique
PATENT ASSIGNEE:
CANON KABUSHIKI KAISHA, (542361), 30-2, 3-chome, Shimomaruko, Ohta-ku,

Tokyo, (JP), (Proprietor designated states: all)
INVENTOR:
Iwamura, Keiichi, c/o Canon Kabushiki Kaisha, 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP)
Yamamoto, Takahisa, c/o Canon Kabushiki Kaisha, 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Beresford, Keith Denis Lewis et al (28273), BERESFORD & Co. 2-5 Warwick Court, High Holborn, London WC1R 5DH, (GB)
PATENT (CC, No, Kind, Date): EP 635956 A2 950125 (Basic)
EP 635956 A3 951206
EP 635956 B1 031022
APPLICATION (CC, No, Date): EP 94305221 940715;
PRIORITY (CC, No, Date): JP 93179232 930720; JP 93179241 930720
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04L-009/22
ABSTRACT WORD COUNT: 105
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200343	989
CLAIMS B	(German)	200343	875
CLAIMS B	(French)	200343	1236
SPEC B	(English)	200343	6361
Total word count - document A			0
Total word count - document B			9461
Total word count - documents A + B			9461

...SPECIFICATION bit sequence for encryption communication comprising:
first generation means for generating a bit sequence based on a first parameter;
second generation means for generating a **random number** sequence **using** a **second parameter** as an initial value; and
modifying means for periodically modifying the first parameter **using** at least part of the random number sequence generated by the second generation means,
the apparatus being characterised in that the first and second generation...

...communication comprising:
a first generation step of sequentially generating a bit sequence based on a first parameter; a second generation step of sequentially generating a **random number** sequence **using** a **second parameter** as an initial value; and
a modifying step of periodically modifying the first parameter using at least part of the random number sequence generated during...

...CLAIMS for encryption communication comprising:
first generation means (13) for generating a bit sequence based on a first parameter;
second generation means (11) for generating a **random number** sequence **using** a **second parameter** as an initial value; and
modifying means for periodically modifying the first parameter **using** at least part of the random number sequence generated by the second generation means (11),
the apparatus being characterised in that the first and second...

...communication comprising:
a first generation step of sequentially generating a bit sequence based on a first parameter;
a second generation step of sequentially generating a **random number** sequence **using** a **second parameter** as an initial value; and
a modifying step of periodically modifying the first parameter using at least part of the random number sequence generated during...

3/3,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00440428
Method of generating a pseudo-random number in a dataprocessing-system, and a system for carrying out the method.
Verfahren zur Erzeugung einer Pseudozufallszahl in einem Datenbearbeitungssystem und ein System zur Ausfuhrung dieses Verfahrens.
Procede de generation d'un nombre aleatoire dans un systeme de traitement de donnees, et systeme mettant en oeuvre un tel procede.
PATENT ASSIGNEE:
BULL CP8, (753211), Rue Eugene Henaff BP 45, F-78190 Trappes, (FR), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
Hazard, Michel, 27, Rue des Harias, F-78124 Mareil sur Mauldre, (FR)
LEGAL REPRESENTATIVE:
Colombe, Michel et al (46243), Direction de la Propriete Intellectuelle BULL SA Poste courrier:LV 59C18 68 route de Versailles, F-78430 Louveciennes, (FR)
PATENT (CC, No, Kind, Date): EP 434551 A1 910626 (Basic)
EP 434551 B1 950208
APPLICATION (CC, No, Date): EP 90403656 901218;
PRIORITY (CC, No, Date): FR 8916768 891219
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: G07F-007/10;
ABSTRACT WORD COUNT: 127

LANGUAGE (Publication,Procedural,Application): French; French; French
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF2	1294
CLAIMS B	(German)	EPBBF2	1114
CLAIMS B	(French)	EPBBF2	1211
SPEC B	(French)	EPBBF2	8934
Total word count - document A			0
Total word count - document B			12553
Total word count - documents A + B			12553

...CLAIMS by modification of at least one memory element of this sub-zone, called the non-specific sub-zone, and in that the first parameter (X), **used** for generating at least one **random number** in combination with the **second parameter** (Y) at the time of the session, is established on the basis, on the one hand of the last modified word in said non-specific...

3/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00224092
Method of secured communications in a telecommunications system.
Verfahren zur gesicherten Ubertragung in einem Ubertragungssystem.
Procede de communication securisee dans un systeme de communication.
PATENT ASSIGNEE:
ICL PLC, (986784), New Century Park P.O. Box 53, Coventry, CV3 1HJ, (GB), (applicant designated states: BE;DE;ES;FR;GR;IT;LU;NL;SE)
INVENTOR:
Phillip, Alexander Schroder, Holly House 31 Highland Road, Wimborne Dorset BH 21 2QL, (GB)
Ozdamar, Mahir, 42 Cogdeane Road Canford Heath, Poole Dorset BH17 9AJ, (GB)
Chopping, Geoffrey, Tregarth Furzehill, Wimborne Dorset BH21 4HD, (GB)

LEGAL REPRESENTATIVE:
  Branfield, Henry Anthony (45871), The General Electric Company plc Patent Department(Wembley Office) Hirst Research Centre East Lane, Wembley, Middlesex HA9 7PP, (GB)
PATENT (CC, No, Kind, Date): EP 225756 A2 870616 (Basic)
EP 225756 A3 890405
EP 225756 B1 930512
APPLICATION (CC, No, Date): EP 86309084 861120;
PRIORITY (CC, No, Date): GB 8530485 851211
DESIGNATED STATES: BE; DE; ES; FR; GR; IT; LU; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/16;
ABSTRACT WORD COUNT: 186

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	595
CLAIMS B	(German)	EPBBF1	541
CLAIMS B	(French)	EPBBF1	646
SPEC B	(English)	EPBBF1	1817
Total word count - document A			0
Total word count - document B			3599
Total word count - documents A + B			3599

...SPECIFICATION possible to encrypt only those messages that apply to a secure call. Bulk Encryption.
The bulk encryption database DEDB, sends routine updates of the message **random variable data** word RV(Q) and the **bulk random variable data** word RVQ encrypted by the rekeying variable data word RKV(1) to **exchange** ExcA. Routine updates of the message random variable data word RV(Q) and the bulk random variable data word RVQ encrypted by the rekeying variable...

...CLAIMS each exchange (EXC A, EXC B) is provided with a store which holds all the user variable data words (RKV A, RKV B) of the **users** connected **to** it, and, each **exchange** (EXC A, EXC B) **is** provided with its own **random** variable **data** word (RV(**Q**)), so **that** when a first user (**SUB** A) makes a secure call to a **second** user (SUB **B**), the first user equipment (SUB A) encrypts a call request **using** its particular user **variable data word** (RKV A) and sends the encrypted data to its own exchange (EXC A), the exchange (EXC A) is provided with equipment for decrypting the call...

...it to the first user (SUB A); the exchange (EXC A) also sends the random variable data word (RV(Q)) to the second user's **exchange** (EXC B) which encrypts it with the user variable data word (RKV **B**) particular to the **second user** (SUB B) and **sends** it **to** the second user (SUB B), **wherein** on **each** occasion where encryption is carried out the frame synchronisation pattern and the spare bits in timeslot zero are not encrypted and wherein a new random...

3/3,K/5 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01116750 **Image available**
OPTIMIZATION OF A BINARY TREE TRAVERSAL WITH SECURE COMMUNICATIONS
OPTIMISATION D'UNE TRAVERSEE D'ARBRE BINAIRE AVEC DES COMMUNICATIONS SURES
Patent Applicant/Assignee:
  MATRICS INC, Columbia Corporate Park 1, 8850 Stanford Boulevard, Suite 3000, Columbia, MD 21045, US, US (Residence), US (Nationality)
Patent Applicant/Inventor:
  POWELL Kevin J, 1202 Cherry Tree Lane, Annapolis, MD 21403, US, US (Residence), US (Nationality)
  SHANKS Wayne E, 1731 Lancaster Street, Baltimore, MD 21231, US, US (Residence), US (Nationality)
  BANDY William R, 2406 Bell Branch Road, Gambrills, MD 21054, US, US

(Residence), US (Nationality)
Legal Representative:
SOKOHL Robert E (et al) (agent), 1100 New York Avenue, N.W., Washington, DC 20005-3934, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200438644 A2 20040506 (WO 0438644)
Application: WO 2003US34036 20031027 (PCT/WO US03034036)
Priority Application: US 2002421050 20021025
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 13237

Fulltext Availability:
Detailed Description

Detailed Description
... is not present.

Such an embodiment is useful when a tag transmits a different second key each time it is negotiated, and/or transmits a **second** key with **variable** length. Any. type of **random bit** pattern generator can be **used** for **random bit** pattern generator 802, including an oscillator, a combination of logic gates, or other type of random bit pattern generator known to persons skilled in the...

3/3,K/6 **(Item 2 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00993956 **Image available**
SYSTEM AND METHOD FOR SECURING A COMMUNICATION CHANNEL
SYSTEME ET PROCEDE PERMETTANT DE SECURISER UN CANAL DE COMMUNICATION
Patent Applicant/Assignee:
WAVE7 OPTICS INC, 1075 Windward Ridge Parkway, Suite 170, Alpharetta, GA 30005, US, US (Residence), US (Nationality)
Inventor(s):
THOMAS Stephen A, 4397 Windsor Oaks Circle, Marietta, GA 30350, US,
BERSON Thomas A, 764 Forest Avenue, Palo Alto, CA 94301, US,
ANTHONY Deven J, 330 Oakridge Terrace, Alpharetta, GA 30005, US,
GONG Guang, 412 Woodrow Drive, Waterloo, Ontario N2T 2V7, CA,
FARMER James O, 3602 Preston Court, Lilburn, GA 30047, US,
Legal Representative:
WIGMORE Steven P (agent), King & Spalding, 191 Peachtree Street, Atlanta, GA 30303-1763, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200323980 A2-A3 20030320 (WO 0323980)
Application: WO 2002US28734 20020910 (PCT/WO US0228734)
Priority Application: US 2001318447 20010910; US 2002388497 20020614
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LU MC NL PT SE SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English

Filing Language: English
Claims Word Count: 19010

Available Text Availability:
Detailed Description

Detailed Description
... transceiver node 120 using equation (1.3) and the first non-secret key parameter 1135 comprising capital letter X of equation (1.0) that is **exchanged** between the parties and the **second** secret key **parameter** small letter y that is not **exchanged** between the parties. In step 1270, the **random number** or nonce 1150 can be decrypted with the newly derived shared secret key. In decision step 1275, it is determined if the decrypted received random...secret key exchange parameter 1140 from small letter y. In step 1430, the shared encryption key can be generated from the first non-secret key **exchange** parameter 1135 and **second** secret key **parameter** . Next, in step 1435, the received **random number** or nonce 1137 can be encrypted with the shared secret key.

In step 1440, an authorization acknowledge message 1145 can be generated and sent to...

3/3,K/7 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00959655 **Image available**
A METHOD AND APPARATUS FOR IMPROVED PSEUDO-RANDOM NUMBER GENERATION
PROCEDE ET APPAREIL DE GENERATION AMELIOREE D'UN NOMBRE PSEUDO-ALEATOIRE
Patent Applicant/Assignee:
NOKIA CORPORATION, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality)
NOKIA INC, 6000 Connection Drive, Irving, TX 75039, US, US (Residence), US (Nationality), (Designated only for: LC)
Inventor(s):
SAARINEN Markku-Juhani, Pihlajatie 50-52 B 31, FIN-00270 Helsinki, FI,
Legal Representative:
FILL Peter N (agent), Morgan & Finnegan, L.L.P., 345 Park Avenue, New York, NY 10154, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200293809 A2-A3 20021121 (WO 0293809)
Application: WO 2002IB1649 20020517 (PCT/WO IB0201649)
Priority Application: US 2001859274 20010517
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE (utility model) DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9889

Available Text Availability:
Detailed Description
Claims

Detailed Description
... The first encrypted result is then concatenated with the first seed value to generate a second encrypted result. The second encrypted result is then encrypted **using** the first key and the block cipher to crenerate a **random number** . A second seed value may then be determined by: (1) encrypting the **second** counter **variable** **using** the key and the block cipher to orenerate a third encrypted result, (2) performing an

exclusive-or operation of the third encrypted result with the...

Claim
... further comprising:
generating the second seed value based on a portion of the fourth output.

35 The method of claim 34, further comprising:
generating a **random number** based on the second key, the **second** counter **variable** and the second seed value. 3 6. The method of claim 35, wherein said generating the **random number** comprises: encrypting said **second** counter **variable using** the second key and a block cipher
to generate an encrypted result;
performing an exclusive-or operation of the encrypted result with the first seed...the counter variable for generating the random number.

66 The method of claim 64, further comprising:
determinincy a seed value based on the key, the **random number** and the counter
variable;
determinina a **second** counter **variable** based on summing the first variable and a
constant; and
generating a second **random number** based on at least the key, the **second** counter **variable** and the seed value.

67 The method of claim 66, wherein said aeneratincr a second **random number** further
ID
comprises:
encrypting said **second** counter **variable using** the key and a block cipher to
generate a first encrypted result;
performing an exclusive-or operation of the first encrypted result with the seed...an exclusive-or operation of the first encrypted result with the first
seed value to generate a second encrypted result;
encrypting the second encrypted result **using** the first key and the block cipher to
generate a **random number** ;
determining a second seed value including:
encrypting said **second** counter **variable using** the key and the
ID
block cipher to generate a third encrypted result;
performing an exclusive-or operation of the third encrypted result with the...or operation of the first encrypted result with the first
ZD
seed value to generate a second encrypted result;
39
encrypting the second encrypted result **using** the first key and the block cipher to
generate a **random number** ;
determining a second seed value including:
encrypting said **second** counter **variable using** the key and the block cipher to generate a third encrypted result;
performing an exclusive-or operation of the third encrypted result with the random...value to generate a second encrypted result;
means for encrypting the second encrypted result usiner the first key and the block
cipher to generate a **random number** ;
means for determining a second seed value including:
means for encrypting said **second** counter **variable using** the key and the
block cipher to generate a third encrypted result;
means for performing an exclusive-or operation of the third encrypted result with...

3/3,K/8 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00735018 **Image available**
METHOD OF SECURING COMMUNICATION
PROCEDE DE COMMUNICATION SECURISE
Patent Applicant/Assignee:
NOKIA NETWORKS OY, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
ANTTI Huima, SMT 10 F 85, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
STYLE Kelda Camilla Karen, Page White & Farrer, 54 Doughty Street, London WC1N 2LS, GB
Patent and Priority Information (Country, Number, Date):
Patent: WO 200048356 A1 20000817 (WO 0048356)
Application: WO 2000EP1061 20000210 (PCT/WO EP0001061)
Priority Application: GB 993123 19990211
Designated States: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9341

Fulltext Availability:
Detailed Description

Detailed Description
... random number messages, first and second security parameter messages, a signature function message, one encoded user identification message and optionally at least two parameters for **use** with a given function message.

A second security method may **use** first and second **random number** messages, first and **second** security **parameter** messages, first and second keys for a given function messages, a signature function message and optionally first and second parameters for **use** with the given function message.
A third security method may **use** first and second **random number** messages, first and **second** security **parameter** messages, first and second keys for given function message, one encoded user identification message, one message to and one message from a third party, one...

9/9/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00768069
Method for secure session key generation
Verfahren zur gesicherten Sitzungsschlusselerzeugung
Procede de generation securisee d'une cle de session
PATENT ASSIGNEE:
AT&T Corp., (589370), 32 Avenue of the Americas, New York, NY 10013-2412, (US), (applicant designated states: BE;CH;DE;GB;IT;LI;LU;NL;SE)
INVENTOR:
Mueller, Kurt H., Hoehenstrasse, 15A, CH-8304 Wallisellen, (CH)
LEGAL REPRESENTATIVE:
Watts, Christopher Malcolm Kelway, Dr. (37391), Lucent Technologies (UK) Ltd, 5 Mornington Road, Woodford Green Essex, IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 720326 A2 960703 (Basic)
EP 720326 A3 990526
APPLICATION (CC, No, Date): EP 95309015 951212;
PRIORITY (CC, No, Date): US 366863 941230
DESIGNATED STATES: BE; CH; DE; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08;

ABSTRACT EP 720326 A2
A symmetric procedure avoids the problems with prior art systems using modifiers with master keys and generates a secure session key from a secret master key and an additional pair of randomly selected signals. The secret master key is known to both parties: one at station A and one at station B. One randomly selected signal of the pair is generated by the party at station A while the other signal in the pair is generated by the party at station B. In one embodiment, a random number signal sent by each one of the parties to the other is encrypted before transmission and decrypted upon reception. Both encryption (at one station) and decryption (at the other station) employ symmetric key cryptographic systems which use the secret master key. The session key is then formed by a commutative combination of both random number signals. (see image in original document)
ABSTRACT WORD COUNT: 166

LEGAL STATUS (Type, Pub Date, Kind, Text):
Examination: 020227 A2 Date of dispatch of the first examination report: 20020111
Examination: 20000112 A2 Date of request for examination: 19991112
Withdrawal: 030226 A2 Date of withdrawal of application: 20021220
Application: 960703 A2 Published application (Alwith Search Report ;A2without Search Report)
Search Report: 990526 A3 Separate publication of the European or International search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	708
SPEC A	(English)	EPAB96	1889
Total word count - document A			2597
Total word count - document B			0
Total word count - documents A + B			2597

SPECIFICATION EP 720326 A2

Technical Field

This invention relates to a method for generating keys for encryption systems and, more particularly, for generating secure session keys for such systems.

Background of the Invention

Changing encryption keys after a certain usage time is an old concept. For example, in the initial key distribution process, an entire table of encryption keys is distributed. Thereafter, each key is used for a

specific time only. Alternatively, a new key can be derived for each session by using mathematical one-way functions such as is done in the Diffie-Hellman algorithm. Finally, with a distributed master key and a series of modifier elements such as a date or time stamp or a counter or the like, one can combine the master key with the modifier elements to generate session keys as needed.

Each of the aforementioned techniques for session key generation suffers from a variety of factors which detract from the appeal of the technique. The first technique requires a fairly large protected memory to store the table of keys. In addition, it requires a significant amount of physical security to keep it from being compromised. The second technique using one-way functions requires powerful processors to compute functions such as discrete logarithms. It also requires a validation of each new key which is generated for the particular session to defy the so-called "person in the middle" attack. The third technique is the most advantageous of the three mentioned. However, if the requirement of unique session keys is imposed, it then becomes necessary for the modifier elements to have a sufficiently long length that maintains an acceptably low probability of repetition. Where data and/or time stamps are used, there are potential security and operational problems arising from clock alignment problems or in allowing communication across different time zones.

Summary of the Invention

A symmetric procedure avoids the problems with prior art systems using modifiers with master keys and generates a secure session key from a secret master key and an additional pair of randomly selected signals. The secret master key is known to both parties: one at station A and one at station B. One randomly selected signal of the pair is generated by the party at station A while the other signal in the pair is generated by the party at station B.

In one embodiment, a random number signal sent by each one of the parties to the other is encrypted before transmission and decrypted upon reception. Both encryption (at one station) and decryption (at the other station) employ symmetric key cryptographic systems which use the secret master key. The session key is then formed by a commutative combination of both random number signals.

In another embodiment, random number signals are sent by each party to the other. Both random number signals are individually decrypted at each station by using symmetric key cryptosystems which employ the secret master key. The session key is then formed by a commutative combination of both decrypted random number signals.

These secure session key generation methods offer the distinct advantage that intercepted, encrypted messages based on the session key cannot be decrypted at a later time even if access to the actual encryption system is gained. Moreover, these methods do not require high speed encryption procedures or special record keeping functions generally associated with other session key generation methods.

Brief Description of the Drawing

A more complete understanding of the invention may be obtained by reading the following description of specific illustrative embodiments of the invention in conjunction with the appended drawing in which:

FIGs. 1 and 2 are illustrative embodiments of a secure session key generation system realized in accordance with the principles of the present invention.

Detailed Description

It is appropriate to provide some cryptology nomenclature at this time. A puzzle can be thought of as a locked box containing a message where the box is secured by a combination lock. Only a bona fide user can probably solve the puzzle. A class of puzzles is known as a cryptographic system or cryptosystem. The process of making a puzzle is known as encryption and the process of solving the puzzle is known as decryption. The puzzle is called ciphertext and the message within the puzzle is called plaintext. The members of a particular cryptosystem are distinguished by a particular key or cryptographic key.

The key to making a specific puzzle (i.e., locking plaintext into

ciphertext) is known as the encryption key. Similarly, the key to solving a puzzle (i.e., recovering the plaintext from the ciphertext) is known as the decryption key. According to the scheme of a particular cryptosystem, a key is used to lock plaintext into ciphertext and that same key can also be used to unlock the ciphertext to retrieve the plaintext. When the encryption key and the decryption key are identical, the cryptosystem is known as a symmetric key cryptosystem.

The notation E(K(sub(M)), R(sub(A))) is the encryption of the signal R(sub(A)) via the symmetric key cryptosystem using master key K(sub(M)). Also, the notation D(K(sub(M)), R(sub(A))) is the decryption of the signal R(sub(A)) via the symmetric key cryptosystem using master key K(sub(M)).

FIG. 1 shows a secure session key generation system realized in accordance with the principles of the present invention. A session key K(sub(S)) is generated mutually and simultaneously at each of two communicating stations, namely station A and station B. Both stations communicate with each other over an insecure communication channel shown by the dashed lines. Session key generation at station A is substantially identical to the session key generation at station B.

The session key generation apparatus at station A includes random number generation element 10, master key element 11, encryption element 12, decryption element 13, combining element 14 and comparison element 16. Similarly, the session key generation apparatus at station A includes random number generation element 20, master key element 21, encryption element 22, decryption element 23, combining element 24 and comparison element 26. Since each station's apparatus is symmetric with that of the other station only station A will be described in detail.

Random number generation element 10 generates a random or pseudo-random sequence of bits as a random number signal R(sub(A)). Signal R(sub(A)) is supplied to encryption element 12 and combining element 14.

Master key element 11 stores the master key K(sub(M)) negotiated at some earlier time between stations A and B or distributed to stations A and B by a key distribution center. That is, both stations A and B have identical master keys. The master key K(sub(M)) is expected to be used over a very long period of time in comparison with the time of use for a session key. Master keys span many sessions or transactions whereas a session key is generally used for a single session or transaction. Master keys can be distributed by couriers or tokens or they can be generated by Diffie-Hellman key exchange or the like.

Encryption element 12 performs the encryption E(K(sub(M)),R(sub(A))) using the master key K(sub(M)) and generates a ciphertext of R(sub(A)) which is transmitted as an outgoing signal to the partner station B. Decryption element 13 receives an incoming signal E(K(sub(M)),R(sub(B))) from station B. The incoming signal corresponds to the ciphertext of the random number signal R(sub(B)) generated by random number generation element 20 and encryption element 22. The latter ciphertext is represented as E(K(sub(M)),R(sub(B))). Decryption element 13 decrypts the incoming signal according to the symmetric key cryptosystem using master key K(sub(M)). The decryption is noted as D(K(sub(M)),E(K(sub(M)),R(sub(B)))) and produces random number signal R(sub(B)).

Station A is now in possession of two random number signals: the one it generated itself R(sub(A)), and the one it received from station B, R(sub(B)). Similarly, station B is now in possession of the same **random number** signals as station A: the one it generated itself, R(sub(B)), and the one it received from station A, R(sub(A)).

Both **random number** signals R(sub(A)) and R(sub(B)) are supplied to combining function element 14 in station A. The combining element performs a commutative combination of the **random number** signals to generate the session key K(sub(S)). Commutative functions which are suitable for use in the combining element satisfy the condition **f (x , y)**=f(y,x) where x and y are R(sub(A)) and R(sub(B)), respectively. Examples of such functions for use in combining element 14 are: linear functions such as addition and addition modulo 2; nonlinear functions such as multiplication and the sum of each variable raised to the same power which is greater than or equal to 2; and one way functions using encryption such as E(K(sub(M)),R(sub(A))+R(sub(B))) or E(R(sub(A)),R(sub(B)))+E(R(sub(B)),R(sub(A))).

$f(x,y) = f(y,x)$ $f(R_A, R_b) = f(R_b, R_a)$.

It is conceivable that R(sub(A)) and R(sub(B)) could be equal. This may or may not lead to a trivial session key depending on the actual function used in combining element 14. In order to avoid such an occurrence, comparing element 16 is used to check whether the random number signals are different. If the signals are different, then the combining element is allowed to process the random number signals. If the signals are the same, then it may be desirable to signal the remote station via a protocol and request a new ciphertext transmission of the random signal.

FIG. 2 shows an alternative embodiment of the secure session key generation system shown in FIG. 1. In this FIG., elements having the same reference numbers as shown in FIG. 1 are identical to those element. The system shown for station A comprises random number generating element 10, master key element 11, decryption elements 13 and 15, combining element 14, and comparing element 16.

For the system in FIG. 2, station A forms random number signal R(sub(A)) from random number generation element 10 and transmits that signal to station B. The random number signal R(sub(A)) is treated as a ciphertext message and supplied to decryption element 15. In a similar manner, station B forms random number signal R(sub(B)) from random number generation element 20 and transmits that signal to station A. Upon reception by station A, the received random number signal R(sub(B)) is treated as a ciphertext message and supplied to decryption element 13.

Decryption element 15 is a symmetric key cryptosystem which responds to the random number signal R(sub(A)) and the master key K(sub(M)) to form the plaintext D(K(sub(M)),R(sub(A))). Also, decryption element 13 is a symmetric key cryptosystem which responds to the random number signal R(sub(B)) and the master key K(sub(M)) to form the plaintext D(K(sub(M)),R(sub(B))). Both plaintext signals are supplied to combining element 14. Combining function 14 accepts both plaintext signals D(K(sub(M)),R(sub(A))) and D(K(sub(M)),R(sub(B))) to generate the session key. Comparing element 16 operates as described earlier to determine whether the plaintext signals are the same or different.

The embodiment shown in FIG. 1 produces a session key which depends only on the random signals R(sub(A)) and R(sub(B)). In the second embodiment (FIG. 2), the session key depends not only on the random number signals R(sub(A)) and R(sub(B)) but also on the master key.

The new methods presented here have a number of desirable properties:

- each station contributes a random input which will influence the common session key;
- preventing decryption of previous message transmissions;
- no need for counters, clocks, timers, time stamps, tables, etc.;
- no record keeping of any sort is required; and
- there is only a soft limit to the number of sessions keys derivable from a specific master key; an increasing number will increase the probability of a potential duplication of an earlier key (so-called "birthday problem") but, in practice, this probability can be kept extremely low.

CLAIMS EP 720326 A2

1. A method of generating a cryptographic session key to a first symmetric key cryptosystem by using a master key signal available to at least first and second parties, the method comprising the steps of:

   forming a first random number signal;

   receiving an incoming signal from one of said parties;

   decrypting the incoming signal via a second symmetric key cryptosystem using the master key signal to recover a second random number signal; and

   generating said cryptographic session key by commutatively combining at least the first and second random number signals.

2. The method as defined in claim 1 wherein the step of generating the cryptographic session key includes the step of comparing the first

and second random number signals to determine whether the random number signals are different from each other.

3. The method as defined in claim 2 wherein the generating step further includes proceeding with generation of the cryptographic session key only when the first and second random number signals differ from each other.

4. The method as defined in claim 1 further including the steps of forming an outgoing signal by encrypting the first random number signal via a third symmetric key cryptosystem using the master key signal and transmitting the outgoing signal to one of the parties.

5. The method as defined in claim 4 further including the steps of:

forming the incoming signal by encrypting the second random number signal via a fourth symmetric key cryptosystem using the master key signal;

transmitting the incoming signal to one of said parties;

decrypting the outgoing signal via a fifth symmetric key cryptosystem using the master key signal to recover the first random number signal; and

generating said cryptographic session key by commutatively combining at least the first and second random number signals.

6. The method as defined in claim 5 wherein the steps of generating the cryptographic session key each include the step of comparing the first and second random number signals to determine whether the random number signals are different from each other.

7. The method as defined in claim 6 wherein the generating steps each further include proceeding with generation of the cryptographic session key only when the first and second random number signals differ from each other.

8. A method of generating a cryptographic session key to a first symmetric key cryptosystem by using a master key signal available to at least first and second parties, the method comprising the steps of:

forming a first signal by decrypting a first random number signal via a second symmetric key cryptosystem using the master key signal;

receiving a second random number signal from one of said parties;

decrypting the second random number signal via a third symmetric key cryptosystem using the master key signal to form a second signal; and

generating said cryptographic session key by commutatively combining at least the first and second signals.

9. The method as defined in claim 8 wherein the step of generating the cryptographic session key includes the step of comparing the first and second signals to determine whether the first and second signals are different from each other.

10. The method as defined in claim 9 wherein the generating step further includes proceeding with generation of the cryptographic session key only when the first and second signals differ from each other.

11. The method as defined in claim 8 further including the steps of forming the first random number signal and transmitting the first random number signal to one of the parties.

12. The method as defined in claim 11 further including the steps of:

forming the second random number signal;

forming the second signal by decrypting the second random number signal via a fourth symmetric key cryptosystem using the master key signal;

transmitting the second random number signal to one of said

parties;

decrypting the first random number signal via a fifth symmetric key cryptosystem using the master key signal to form the first signal; and

generating said cryptographic session key by commutatively combining at least the first and second random number signals.

13. The method as defined in claim 12 wherein the steps of generating the cryptographic session key each include the step of comparing the first and second signals to determine whether the first and second signals are different from each other.

14. The method as defined in claim 13 wherein the generating steps each further include proceeding with generation of the cryptographic session key only when the first and second signals differ from each other.

File 347:JAPIO Nov 1976-2004/Jan(Updated 040506)
(c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200434
(c) 2004 Thomson Derwent

Set	Items	Description
S1	16115	(RANDOM? OR PSEUDORANDOM?)(3W)(NUMBER? ? OR NUMERAL? ? OR VALUE? ? OR DATA OR INFORMATION OR FIGURE? ? OR DIGIT? ? OR INTEGER? ? OR BIT? ? OR BYTE? ? OR CONTENT OR AMOUNT? ? OR QUANTIT???)
S2	5355	(SECOND? OR 2ND)(2W)(VARIABLE OR PARAMETER OR ATTRIBUTE OR LETTER OR PLACEHOLDER OR PLACE()HOLDER)
S3	3	S1(7N)S2(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR INCORPORAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING OR IN(1W)PLACE)
S4	103	S1(7N)(B OR Y)(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR INCORPORAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING OR IN(1W)PLACE)
S5	22	S4 AND FUNCTION? ?
S6	1	S4 AND F(1W)(A()B OR X()Y)
S7	21	S5 NOT (S3 OR S6)

3/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015712980 **Image available**
WPI Acc No: 2003-775180/200373
Method for creating card user number for electronic commerce,device, and system for payment using the same
Patent Assignee: KIM D W (KIMD-I)
Inventor: KIM D W; KIM J U
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2003050576	A	20030625	KR 200181047	A	20011219	200373	B

Priority Applications (No Type Date): KR 200181047 A 20011219
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2003050576	A		1	G06F-017/60	

Abstract (Basic): KR 2003050576 A
NOVELTY - A method for creating a card user number for an electronic commerce, a device and system for a payment using the same are provided to update and create a card user number in each transaction.
DETAILED DESCRIPTION - A terminal key number and key data are set by combining a partial portion of wireless communication terminal number(S100). One random number is selected out of many random numbers stored in a memory based on a nonlinear ASCII array stored in accordance with the key data(S110). The terminal key number and key data are used for the first input variable of the first encoding algorithm for a card user number creation. The terminal key number and the **random number** are **used** for the **second** input **variable** . The first input variable and the **second variable** are applied to the first encoding algorithm, and the first encoding data are created(S120-S130). Each digit position of the first encoding data is changed based on mix data(S140). An additional vector is added to mixed data, and the added result value is modulated into duosexadecimal(S150). A value of check data is set(S160). The second encoding data including the check data value are calculated. All values of a variable field are calculated. The second encoding data of 10-digit is substituted with a non-linear array value, and the final variable field data are created(S170,S180).
pp; 1 DwgNo 1/10
Title Terms: METHOD; CARD; USER; NUMBER; ELECTRONIC; DEVICE; SYSTEM; PAY
Derwent Class: T01
International Patent Class (Main): G06F-017/60
File Segment: EPI

3/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010770542 **Image available**
WPI Acc No: 1996-267496/199627
XRPX Acc No: N96-224939
Game for forming words upon board to entertain and educate players - includes board simulating various cross-word puzzle configurations upon which number of tiles can be positioned to form words
Patent Assignee: BRUECKNER J L (BRUE-I)
Inventor: BRUECKNER J L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5520394	A	19960528	US 95429852	A	19950424	199627	B

Priority Applications (No Type Date): US 95429852 A 19950424

Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
US 5520394 A 9 A63F-003/00

Abstract (Basic): US 5520394 A

The board game includes providing a game board divided into a number off blank squares and including a number of shaded squares arranged in a pattern relative to the game board. The next step is providing a number of letter tiles being of a first colour on a first side of it and being of a second colour on a second side of it.

The next step is selecting a first player for initiating the game and for utilizing the first colour of the letter tiles, and selecting a second player for utilizing the second colour of the letter tiles, and randomly selecting a number of the letter tiles by the first player for **use** in the first colour as first colour letter tiles. The next step is **randomly** selecting a **number** of the letter tiles by the second player for **use** in the second colour as **second** colour **letter** tiles, and forming a word by the first player from the first colour letter tiles by a word forming method selected from the group.

ADVANTAGE - The game entertains and educates players.

Dwg.8/8

Title Terms: GAME; FORMING; WORD; BOARD; PLAY; BOARD; SIMULATE; VARIOUS; CROSS; WORD; PUZZLE; CONFIGURATION; NUMBER; TILE; CAN; POSITION; FORM; WORD

Derwent Class: P36

International Patent Class (Main): A63F-003/00

File Segment: EngPI

3/5/3 **(Item 3 from file: 350)**

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

[illegible]9890

WPI Acc No: 1983-J8093K/198326

XRPX Acc No: N83-114635

Controlling of scrambling and unscrambling in pay TV system - is dependent on variable different for each type of programme and periodically e.g. monthly and variable changing from field to field

Patent Assignee: NORTHERN TELECOM LTD (NELE)

Inventor: AMINETZAH Y J

Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 4388643	A	19830614				198326 B
CA 1160734	A	19840117				198408

Priority Applications (No Type Date): US 81251085 A 19810406

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
US 4388643 A 9

Abstract (Basic): US 4388643 A

The control consists of storing a subscriber number at a subscriber station and recurrently transmitting to the subscriber station a first variable encoded in dependence upon the subscriber number. The variable is decoded at the subscriber station using the stored subscriber number, and the variable is stored before or after decoding. The video signal is scrambled in dependence upon the first variable and a second variable.

The second variable is transmitted to the subscriber station simultaneously with transmission of the scrambled video signal. At the subscriber station the video signal is unscrambled in dependence upon the decoded stored first variable and the transmitted **second variable** . The first variable may be produced **using** a **random number** generator and the second by a pseudo- **random number** generator. Encryption and programme data may be sent to the subscriber via a telephone link.

06310472 **Image available**
USER CERTIFYING SYSTEM

PUB. NO.: 11-252070 [JP 11252070 A]
PUBLISHED: September 17, 1999 (19990917)
INVENTOR(s): HANEDA TOMOSHI
TANAKA TOSHIAKI
APPLICANT(s): KDD CORP
APPL. NO.: 10-063867 [JP 9863867]
FILED: March 02, 1998 (19980302)
INTL CLASS: H04L-009/32; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a system satisfying zero knowledge and reducing the number of times of communication by generating an integer and a random number of the side of a certifier, transmitting them to a verifier, generating a random number on the side of the verifier, transmitting two codes to the certifier, performing transmission from the certifier to the verifier when a specified relation is established between the codes, and using any specified code as a challenge random number when the specified relation is confirmed between the codes.

SOLUTION: The sertifier generates a random number (a) through a random number (a) generator 101 and transmits a code A = function F (G, a) generated by a code computing element 13 while **using** an integer G and this **random number** (a) and that integer G to the verifier. The certifier generates a **random number** (**b**) through a **random number** (**b**) generator 2-1 and transmits a code **B** = function F (G, **b**) generated by a code computing element 2-2 while **using** this **random number** (**b**), code A and integer G and a code X = function **F** (**A** , **b**) to the certifier. The certifier certifies whether the condition of code X = function F (B, a) is established or not through a verifier 1-4. When this condition is not established, this protocol is interrupted.

integer (verifier) →

$A = F(G, a)$

$B = F(G, b)$

$X = F(A, b)$

```
File   8:Ei Compendex(R) 1970-2004/May W4
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/May
         (c) 2004 ProQuest Info&Learning
File  65:Inside Conferences 1993-2004/May W5
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/May W4
         (c) 2004 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2004/May W2
         (c)2004 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2004/May W5
         (c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2004/May W4
         (c) 2004 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2004/May W5
         (c) 2004 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Apr
         (c) 2004 The HW Wilson Co.
File 266:FEDRIP 2004/Apr
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2004/May W3
         (c) 2004 FIZ TECHNIK
File 104:AeroBase 1999-2004/Apr
         (c) 2004 Contains copyrighted material
File  62:SPIN(R) 1975-2004/Apr W2
         (c) 2004 American Institute of Physics
File 239:Mathsci 1940-2004/Jul
         (c) 2004 American Mathematical Society

Set     Items   Description
S1      28639   (RANDOM? OR PSEUDORANDOM?)()(NUMBER? ? OR NUMERAL? ? OR VA-
             LUE? ? OR DATA OR INFORMATION OR FIGURE? ? OR DIGIT? ? OR INT-
             EGER? ? OR BIT? ? OR BYTE? ? OR CONTENT OR AMOUNT? ? OR QUANT-
             IT???)
S2       6134   (SECOND? OR 2ND)(2W)(VARIABLE OR PARAMETER OR ATTRIBUTE OR
             LETTER OR PLACEHOLDER OR PLACE()HOLDER)
S3          0   S1(7N)S2(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR INCORPO-
             RAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING OR IN(-
             1W)PLACE)
S4         74   S1(7N)(B OR Y)(7N)(REPLAC? OR SUBSTITUT? OR INSERT??? OR I-
             NCORPORAT? OR SWAP???? OR EXCHANG??? OR USE OR USED OR USING -
             OR IN(1W)PLACE)
S5         12   S4 AND FUNCTION? ?
S6          0   S4 AND F(1W)(A()B OR X()Y)
S7         10?  RD S5 (unique items)
```

7/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06380900 E.I. No: EIP03197467096
Title: Random difference equations: An asymptotical result
Author: Chamayou, J.F.; Dunau, J.L.
Corporate Source: Lab.de statistique et probabilites Universite Paul Sabatier, Toulouse, Cedex F-31062, France
Source: Journal of Computational and Applied Mathematics v 154 n 1 May 1 2003. p 183-193
Publication Year: 2003
ISSN: 0377-0427
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0305W3
Abstract: we give a description of the model U//n = X//n(1 + U//n//-//1) for n greater than 1 in the case where the X//i are i.i.d random variables with density alphax**alpha**-**1 on left bracket 0,1 right bracket , (alpha greater than 0). We **use** it to generate recursively Dickman **pseudorandom numbers** (alpha = 1) and to simulate shot noise. copy 2003 Elsevier Science **B** .V. All rights reserved. 18 Refs.
Descriptors: Difference equations; Random processes; Recursive **functions** ; Shot noise; Mathematical models
Identifiers: Random difference equations
Classification Codes:
921.6 (Numerical Methods); 922.1 (Probability Theory); 701.1 (Electricity, Basic Concepts & Phenomena)
921 (Applied Mathematics); 922 (Statistical Methods); 701 (Electricity & Magnetism)
92 (ENGINEERING MATHEMATICS); 70 (ELECTRICAL ENGINEERING, GENERAL)

7/5/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6431108 INSPEC Abstract Number: C2000-01-1260-015
Title: Error reduction for extractors
Author(s): Raz, R.; Reingold, O.; Vadhan, S.
Author Affiliation: Dept. of Appl. Math. & Comput. Sci., Weizmann Inst. of Sci., Rehovot, Israel
Conference Title: 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039) p.191-201
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1999 Country of Publication: USA xiv+668 pp.
ISBN: 0 7695 0409 4 Material Identity Number: XX-1999-03193
U.S. Copyright Clearance Center Code: 0 7695 0409 4/99/$10.00
Conference Title: 40th Annual Symposium on Foundations of Computer Science
Conference Sponsor: IEEE Comput. Soc. Tech. Committe on Math. Found. Comput
Conference Date: 17-19 Oct. 1999 Conference Location: New York City, NY, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: An extractor is a **function** which extracts (almost) truly random bits from a weak random source, using a small number of additional random bits as a catalyst. We present a general method to reduce the error of any extractor. Our method works particularly well in the case that the original extractor extracts up to a constant **function** of the source min-entropy and achieves a polynomially small error. In that case, we are able to reduce the error to (almost) any epsilon , using only O(log(1/epsilon)) additional truly random bits (while keeping the other parameters of the original extractor more or less the same). In other cases (e.g. when the original extractor extracts all the min-entropy or achieves only a constant error), our method is not optimal but it is still quite efficient and leads to improved constructions of extractors. Using our method, we are

able to improve almost all known extractors in the case where the error required is relatively small (e.g. less than a polynomially small error). In particular, we apply our method to the new extractors of L. Trevisan (1999) and R. Raz et al. (1999) to obtain improved constructions in almost all cases. Specifically, we obtain extractors that work for sources of any min-entropy on strings of length n which (a) extract any 1/n/sup gamma / fraction of the min-entropy **using** O[log n+log(1/ epsilon)] truly **random bits** (for any gamma >0), (**b**) extract any constant fraction of the min-entropy **using** O[log/sup 2/n+log(1/ epsilon)] truly random bits, and (c) extract all the min-entropy using O[log/sup 3/n+log n.log(1/ epsilon)] truly random bits. (10 Refs)

Subfile: C

Descriptors: computational complexity; errors; **functions** ; minimum entropy methods

Identifiers: extractor error reduction; source min-entropy; polynomially small error; truly random bits; extractor constructions; strings; extractor **functions** ; weak random source; additional random bits

Class Codes: C1260 (Information theory); C4240C (Computational complexity); C1180 (Optimisation techniques)

7/5/3 (Item 2 from file: 2)

4900848 INSPEC Abstract Number: A9507-9850K-009

Title: Non-linear clustering in the cold plus hot dark matter model

Author(s): Bonometto, S.A.; Borgani, S.; Ghigna, S.; Klypin, A.; Primack, J.R.

Author Affiliation: Dipartimento di Fisica, Milan Univ., Italy

Journal: Monthly Notices of the Royal Astronomical Society vol.273, no.1 p.101-21

Publication Date: 1 March 1995 Country of Publication: UK

CODEN: MNRAA4 ISSN: 0035-8711

U.S. Copyright Clearance Center Code: 0035-8711/95/$11.00

Language: English Document Type: Journal Paper (JP)

Treatment: Theoretical (T)

Abstract: Finds out if hierarchical scaling, observed in galaxy clustering, can be dynamically explained by studying N-body simulations. Previous analyses of dark matter (DM) particle distributions indicated heavy distortions with respect to the hierarchical pattern. The authors describe how such distortions are to be interpreted and why they can be fully reconciled with the observed galaxy clustering. This aim is achieved by using high-resolution (512/sup 3/ gridpoints) particle-mesh N-body simulations to follow the development of non-linear clustering in a Omega =1 universe, dominated either by cold dark matter (CDM) or by a mixture of cold+hot dark matter (CHDM) with Omega /sub cold/=0.6, Omega /sub hot/=0.3 and Omega /sub baryon/=0.1; a simulation box of side 100 Mpc (h=0.5) is used . The authors analyse two CHDM realizations with biasing factor **b** =1.5 (COBE normalization), starting from different initial **random numbers** , and compare them with CDM simulations with **b** =1 (COBE-compatible) and **b** =1.5. The authors evaluate high-order correlation **functions** and the void probability **function** . Correlation **functions** are obtained from both counts in cells and counts of neighbours. The analysis is carried out for DM particles and for galaxies identified as massive haloes of the evolved density field. The authors confirm that clustering of DM particles systematically exhibits deviations from hierarchical scaling, although the deviation decreases somewhat in redshift space. (68 Refs)

Subfile: A

Descriptors: clusters of galaxies; cosmology; dark matter

Identifiers: cold plus hot dark matter model; hierarchical scaling; nonlinear galaxy clustering; dark matter particle distributions; large scale structure; particle-mesh N-body simulations; early Universe; box model; correlation **functions** ; void probability **function** ; cell counts; neighbour counts; massive haloes; evolved density field; galaxy formation; redshift space

Class Codes: A9850K (Groups, clusters, and superclusters of galaxies); A9880B (Origin and early evolution of the Universe); A9850B (Origin, evolution, and ages of galaxies)

7/5/4 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

4665241 INSPEC Abstract Number: A9412-0545-002, B9406-0170E-012
Title: Practical time-series analysis with multifractal methods
Author(s): Klement, S.; Kratky, K.W.; Nittmann, J.
Author Affiliation: Campusbased Eng. Center, Digital Equipment Corp., GebH, Vienna, Austria
Journal: Fractals vol.1, no.3 p.735-43
Publication Date: Sept. 1993 Country of Publication: Singapore
CODEN: FRACEG ISSN: 0218-348X
Conference Title: Fractals in Natural Sciences
Conference Date: 30 Aug.-2 Sept. 1993 Conference Location: Budapest, Hungary
Language: English Document Type: Conference Paper (PA); Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: Time-series data of various origins are studied by analyzing their corresponding multifractal f(alpha)-spectra which are obtained by use of the so-called canonical method. The classes of data samples under investigation include: (a) airborne particle count data taken from an industrial cleanroom environment; (**b**) data generated by **use** of a (pseudo-) **random number** generator; and (c) data resulting from the iteration of the logistic map for the value r=4.0 of the control parameter, thus exhibiting chaotic behavior. From the resulting multifractal spectra, typical features of the f(alpha)-curve can be identified in relation to the corresponding class of original data. These findings can be of interest for various purposes. One application under consideration is the processing of microcontamination particle data recorded in high-quality cleanrooms. These are of great importance to the increasing miniaturization of semiconductor devices. In processing microcontamination particle data, the multifractal analysis can help to extract significant information from an enormous number of data to compress these data into a reasonable quantity. Another interesting aspect can be found in using the multifractal spectrum as a possible instrument for estimating the quality and performance of a random number generator. (9 Refs)
Subfile: A B
Descriptors: chaos; clean rooms; random **functions** ; time series
Identifiers: time-series; multifractal methods; multifractal f(alpha)-spectra; canonical method; airborne particle count data; cleanroom; random number generator; logistic map; chaotic behavior; f(alpha)-curve
Class Codes: A0545 (Theory and models of chaotic systems); A0250 (Probability theory, stochastic processes, and statistics); B0170E (Production facilities and engineering); B0240 (Probability and statistics)

7/5/5 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

00565668 JICST ACCESSION NUMBER: 88A0127369 FILE SEGMENT: JICST-E
A study of pseudo- random number **generation subject to any probability distribution. Estimation of probability density** function using B **spline** function .
OKUMURA HIROZO (1); KITAOKA MASATOSHI (1)
(1) Kanagawa Univ.
Nippon Keiei Kogakkai Shuki Kenkyu Taikai Yokoshu, 1987, VOL.1987, PAGE.137-138, FIG.6, REF.3
JOURNAL NUMBER: F0876BAD
UNIVERSAL DECIMAL CLASSIFICATION: 658.562.012.7 65.012.122
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan

DOCUMENT TYPE: Conference Proceeding
ARTICLE TYPE: Short Communication
MEDIA TYPE: Printed Publication
DESCRIPTORS: probability distribution; random number generation; spline **function** ; probability density; **function** (mathematics); sample(statistics); estimation; histogram; pseudorandom number; sequence; Monte Carlo method
BROADER DESCRIPTORS: distribution; signal generation; generation; mapping(mathematics); density; diagram and table; random number
CLASSIFICATION CODE(S): KB04030W; KA03010Q

7/5/6 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

12266312 PASCAL No.: 95-0495846
The relationship of the 6-min walk test to maximal oxygen consumption in transplant candidates with end-stage lung disease
CAHALIN L; PAPPAGIANOPOULOS P; PREVOST S; WAIN J; GINNS L
Massachusetts gen. hosp., physical therapy serv., lung transplant program , Boston MA 02114, USA
Journal: Chest, 1995, 108 (2) 452-459
ISSN: 0012-3692 CODEN: CHETBF Availability: INIST-7627; 354000053927590320
No. of Refs.: 34 ref.
Document Type: P (Serial) ; A (Analytic)
Country of Publication: USA
Language: English
Study objective : To assess the relationship of distance ambulated during the 6-min walk test (6'WT) to maximal oxygen consumption (Vo SUB 2 max). Design : Multivariate analysis of patient characteristics to Vo SUB 2 max. Setting : Pre-lung transplant evaluation. Patients : 60 patients (22 men, 38 women ; mean age, 44 years) with end-stage lung disease (mean FEV SUB 1 and forced vital capacity of 0.97 and 1.93, respectively). Measurements and results : The 6'WT was performed on a level hallway surface, and Vo SUB 2 max was obtained during maximal cycle ergometry exercise testing with respiratory gas analysis. Multivariate analysis of patient characteristics (age, sex, weight, FEV SUB 1 , FVC, diffusing capacity for carbon monoxide (Dco), 6'WT distance ambulated, number of rests per 6'WT, and the maximal heart rate, blood pressure, rate-pressure product, respiratory rate, oxygen saturation, rating of perceived exertion, and amount of supplemental oxygen **used** during the 6'WT) was performed on two groups of 30 patients each (group A or **B**) who were randomly assigned to either group by a process of random selection **using** a computer-generated **random numbers** program. Distance ambulated was the strongest independent predictor of Vo SUB 2 max (r=0.73 ; p<0.0001) in both groups, and adding age, weight, and pulmonary **function** test results (FVC, FEV SUB 1 , and Dco) to the regression equation increased the correlation coefficient to 0.83. Because of the significant correlation of distance ambulated during the 6'WT to Vo SUB 2 max, the prediction equation obtained from the multivariate analysis of group A, Vo SUB 2 max= 0.006xdistance (feet) +3.38, was used to estimate the Vo SUB 2 max of the group B patients. No significant difference was observed between the estimated (x +- SD=8.9 +- 2.4 mL/kg/min) and observed (x +- SD=9.4 +- 3.8 mL/kg/min)Vo SUB 2 max (mean difference, 0.5 mL/kg/min ; SD of the difference=2.88). Conclusions : The distance ambulated during a 6'WT can predict

English Descriptors: Respiratory failure; Exercise tolerance test; Moving way; Tolerance; Physical exercise; Distance; Oxygen consumption; Exploration; Relation; Human
Broad Descriptors: Respiratory disease; Appareil respiratoire pathologie; Aparato respiratorio patologia

French Descriptors: Insuffisance respiratoire; Epreuve effort; Tapis roulant; Tolerance; Exercice physique; Distance; Consommation oxygene; Exploration; Relation; Homme

Classification Codes: 002B11D

7/5/7 **(Item 1 from file: 99)**
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1293187 H.W. WILSON RECORD NUMBER: BAST96015402
Smooth B-spline illumination maps for bidirectional ray tracing
Redner, Richard A; Lee, Mark E; Uselton, Samuel P
ACM Transactions on Graphics v. 14 (Oct. '95) p. 337-62
DOCUMENT TYPE: Feature Article ISSN: 0730-0301 LANGUAGE: English
RECORD STATUS: New record

ABSTRACT: The use of smooth B-spline illumination maps for bidirectional ray tracing is discussed. In an effort to generate more realistic computer-generated images, there has been an increase over the last few years in the **use** of distributed light sources in computer graphics. **B** -spline lighting **functions** , which can be defined as weighted probability density **functions** , can be estimated from **random data** and may be employed in bidirectional distributed ray tracing programs and radiosity oriented algorithms. The **use** of **B** -spline lighting **functions** in a bidirectional ray tracing system capable of rendering images that show dispersion and the concentration of light by translucent objects is demonstrated.

DESCRIPTORS: Density **function** ; Spline **functions** ; Ray tracing--
Mathematical models;

7/5/8 **(Item 1 from file: 239)**
DIALOG(R)File 239:Mathsci

03260653 MR 2002d#65011
A heuristic algorithm for stochastic root finding.
The 5th Conference of the Association of Asian-Pacific Operations Research Societies (Singapore, 2000).
Chen, Huifen (Department of Industrial Engineering, Chung Yuan Christian University, Chungli 32023, Taiwan (R.O.C.))
Chen, Hungshen
Corporate Source Codes: RC-CYCH-IE
Asia-Pacific J. Oper. Res.
Asia-Pacific Journal of Operational Research, 2001, 18, no. 1, 13--22. ISSN: 0217-5959
Language: English Summary Language: English
Document Type: Journal
Journal Announcement: 200115
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (19 lines)
A computational algorithm is described and tested for solving the n-dimensional stochastic root-finding problem (SRFP) in which estimates are available only for the n-dimensional **function** values. Specifically, to approximately solve $G(x)=\gamma$ where $x,\gamma\in{\bf R}\sp n,\ y(x,\omega)=\gamma$ is solved for x where $ **y** (x,\omega)$ is an estimate of $G(x)$ **using** pseudo- **random numbers** $\omega\in{\bf R}\sp m$ and where the estimate $ **y** (x,\omega)$ improves as m increases. In the iterative numerical method described, a sequence of approximations $\{x\sb k\}\sb {k=1}\sp \infty$ is essentially obtained using the following procedure: $y(x\sb 1,\omega\sb 1)=\gamma$ is solved using Broyden's method for $\omega\sb 1\in{\bf R}\sp {m\sb 1},\ y(x\sb 2,\omega\sb 2)=\gamma$ is solved using Broyden's method for $\omega\sb 2\in{\bf R}\sp {m\sb 2}$ where $m\sb 2>m\sb 1$ and the calculations continue until a weighted average of the values $x\sb k$, for $k=1,2,\dots$, converges. Numerical results are presented for the method. The results indicate that computational time increases substantially with dimension n.
Reviewer: Allen, Edward J. (1-TXT-MS)

Review Type: Signed review
Descriptors: *65C50 -Numerical analysis-Probabilistic methods, simulation and stochastic differential equations (For theoretical aspects, see 68U20 and 60H35)-Other computational problems in probability ; 60H35 -Probability theory and stochastic processes (For additional applications, see 11Kxx, 62-XX, 90-XX, 91-XX, 92-XX, 93-XX, 94-XX)-Stochastic analysis (See also [illegible]65)-Computational methods for stochastic equations (See also 65C30)

7/5/9 **(Item 2 from file: 239)**
DIALOG(R)File 239:Mathsci

03058751 MR 2000i#65007
Adaptive schemes of the Monte Carlo method of an increased order of accuracy.
Ivanov, V. M. (Department of Mathematics, St. Petersburg Technical University, 195257 St. Petersburg, Russia)
Korenevskii, M. L. (Department of Mathematics, St. Petersburg Technical University, 195257 St. Petersburg, Russia)
Kulchitskii, O. Yu. (Department of Mathematics, St. Petersburg Technical University, 195257 St. Petersburg, Russia)
Corporate Source Codes: RS-STPP; RS-STPP; RS-STPP
Dokl. Akad. Nauk
Rossiiskaya Akademiya Nauk. Doklady Akademii Nauk, 1999, 367, no. 5, 590--593. ISSN: 0869-5652
Language: Russian
Document Type: Journal
Journal Announcement: 200005
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (13 lines)
Adaptive schemes are proposed for Monte Carlo integration. The estimator $$\widehat{J}\sb{N}=\sum\sb{i=1}\sp{N}\alpha\sb{i}\frac{f\left(x\sb{i}\right)}{p \sb{i}\left(x\sb{i}\right)},\quad \alpha\sb{i}\ge 0,\ \sum\sb{i=1}\sp{N}\alpha\sb{i}=1,$$ for the integral $ J\!=\!\int\sb{a}\sp{b}f\left(x\right)dx $ is successively constructed. Here, $p\sb{i}$, $i=1,\cdots,N$, are density **functions** with support (a, b), and $x\sb{i}$, $i=1,\cdots,N$, are respectively $p\sb{i}$-distributed **random numbers** . **Using** the first k generated **random numbers** as knots of the division of the interval $(a, **b**)$, the density **function** $p\sb{k+1}$ is obtained by a piecewise approximation of the **function** f. Mean-square convergence of $\widehat{J}\sb{N}$ to J is proved.
Reviewer: Blaga, Petru P. (R-CLUJ)
Review Type: Signed review
Descriptors: *65C05 -Numerical analysis-Probabilistic methods, simulation and stochastic differential equations (For theoretical aspects, see 68U20 and 60H35)-Monte Carlo methods

7/5/10 **(Item 3 from file: 239)**
DIALOG(R)File 239:Mathsci

01155434 MR 27##5352
Application of the $\omega \sp{2}$-distribution for an error bound in evaluating integrals by the Monte-Carlo method.
Sobol, I. M.
Z. Vycisl. Mat. i Mat. Fiz.
1962, 2, 717--723
Language: Russian
Document Type: Journal
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: MEDIUM (25 lines)
Let $\xi\sb 1,\cdots,\xi\sb N$ be values of random variables uniformly distributed on the interval $[0,1]$. The quantity $m\sb n(f)=N\sp{-1}\sum\sb{i=1}\sp Nf(\xi\sb i)$ provides a Monte Carlo estimate of $Mf=\int\sb 0\sp 1f(x)\,dx$. Let $\delta\sb N=m\sb N(f)-Mf$. If $f\in L\sb 2$, let $Df=\int\sb 0\sp 1f\sp 2(x)\,dx-(Mf)\sp 2$. Since $\delta\sb

N/(Df/N)\sp {1/2}$ is asymptotically normally distributed $N(0,1)$, it provides a probabilistic error bound for $m\sb N(f)$ as an estimator of Mf. The bound is valid for any **function** $f\in L\sb 2$, but only for one **function** .

Let $S\sb N(x)$ be the number of points $\xi\sb i<x$. Let $F\sb N(x)=S\sb N(x)/N$. Then $\omega\sb N{}\sp 2=N\int\sb 0\sp 1[x-F\sb N(x)]\sp 2\,dx$ is a Mises-Smirnov statistic. Let $W\sb 2{}\sp {(1)}(L)$ be the class of f such that $\int\sb 0\sp 1[f'(x)]\sp 2\,dx\leq L\sp 2$. The author shows that for all $f\in W\sb 2{}\sp {(1)}(L)$, one has $\vert \delta\sb N\vert \leq L\surd(\omega\sb N{}\sp 2/N)$.

The last bound is valid uniformly for all f in $W\sb 2{}\sp {(1)}(L)$. The author uses it to give error bounds for the simultaneous estimation of $g(y)=\int\sb 0\sp 1F(x,y)\,dy$ by $\gamma\sb N(y)=N\sp {-1}\sum\sb {i=1}\sp Nf(\xi\sb i, **y**)$, for $0\leq **y** \leq 1$, where the same **random numbers** $\{\xi\sb i\}$ are **used** for all $ **y** $. Moreover, dividend differences of the $\gamma\sb N(y)$ can be used to estimate $g'(y)$, with error bounds, provided F is smooth enough.

Search Results

Search Results for: **[(replac* or substitut* or insert* or incorporat* or swap* or exchang* or use or used or using or in place) <near/10> (random number or random value or random integer or random data or random bit or random byte) <near/10> (b or y) <near/10> function]**
Found **1** of **134,837 searched.**

Search within Results

go > Advanced Search

> Search Help/Tips

Sort by: **Title** **Publication** **Publication Date** **Score** Binder

Results 1 - 1 of 1 **short listing**

1 Correlation-induction techniques for estimating quantiles in simulation experiments 95%
Athanassios N. Avramidis , James R. Wilson
Proceedings of the 27th conference on Winter simulation December 1995

Results 1 - 1 of 1 **short listing**

Try the *new* Portal design

Give us your opinion after using it.

Search Results

Nothing Found

Your search for **[(replac* or substitut* or insert* or incorporat* or swap* or exchang* or use or used or using or in place) <near/10> (random number or random value or random integer or random data or random bit or random byte) <near/10> (second variable or 2nd variable)]** did not return any results.

You may revise it and try your search again below or click advanced search for more options.

(replac* or substitut* or insert* or incorporat* or swap* or exchang* or use or used or using or in place) <near/10> (random number or random value or random integer or random data or random bit or random byte) <near/10> (second variable or 2nd variable)

SEARCH **[Advanced Search]** **[Search Help/Tips]**

Complete Search Help and Tips

The following characters have specialized meaning:

Special Characters	Description
, ( ) [	These characters end a text token.
= > < !	These characters end a text token because they signify the start of a field operator. (! is special: != ends a token.)
` @ \Q < { [!	These characters signify the start of a delimited token. These are terminated by the end character associated with the start character.